Doc Code: AP.PRE.REQ

PTO/SB/33 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
I0046.0162	
Application Number	**Filed**
10/735,517	December 11, 2003
First Named Inventor	
Gernot Eckstein et al.	
Art Unit	**Examiner**
2436	C. Johnson

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant /inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 38,395

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. _____

/Laura C. Brutman/
Signature

Laura C. Brutman
Typed or printed name

(212) 277-6592
Telephone number

March 2, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.

ATTACHMENT TO PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 1, 3, 5, 7, 9, and 10 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Niessen et al. (U.S. Patent No. 5,367,638; hereinafter "Niessen") in view of Dias (U.S. Patent No. 4,855,690). Claims 6 and 8 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Niessen and Dias in view of Read et al. (U.S. Patent No. 5,353,243; hereinafter "Read").

Appellant respectfully traverses the prior art rejections for the following reasons.

The present application is concerned with techniques of preventing unauthorized external access to the operation of integrated digital circuits. The application is particularly concerned with countermeasures against so-called side-channel attacks which are performed by unauthorized parties for analyzing integrated circuits, for example, for analyzing coding algorithms performed by a cryptocoproccessor.

In accordance with a first aspect of the application, the external detection of operations in a digital integrated circuit comprising an asynchronous circuit is prevented by time-varying a supply voltage of the asynchronous circuit to time-shift the execution of operations within the asynchronous circuit, wherein the time-variation of the supply voltage takes place in a random way, as recited in independent claim 1.

In accordance with a second aspect of the application, a digital integrated circuit comprises an asynchronous circuit and means for time-varying a supply voltage of the asynchronous circuit to time-shift the execution point of operations within the asynchronous circuit, wherein the means for time-varying the supply voltage comprises a random number generator, as recited in independent claim 3.

The Examiner concedes on page 4, lines 2-3 of the final Office Action that Niessen does not disclose that time variation takes place in a random way. In an attempt to make up for this deficiency, the Examiner applies Dias. The Examiner asserts at page 2, last paragraph, fourth line, of the final Office Action, that "The 103 combination of Niessen and Dias proposes the inclusion of

the random number generation feature of Dias and using the concept of this feature to control the timing of voltage within the already established features or limitations of the Niessen invention."

The Examiner continues by asserting that "Even with a random signal at the filling degree signal the filling should still occur." The Examiner asserts on page 3, first sentence, of the final Office Action that in his opinion there is no indication that the desired filling degree control of Niessen would no longer work (when replacing the feedback-control of the filling degree of Niessen by the random number generation feature of Dias).

Appellant respectfully disagrees with the Examiner's position.

Niessen discloses a digital data processing circuit in an apparatus comprising a data source which feeds a buffer for intermediate storage of data and subsequent outputting thereof and comprising a feedback circuit which, under control of a filling degree signal of the buffer, dynamically controls the data handling rate of the data source (see column 1, lines 7-12).

The digital apparatus comprises a data source including an integrated digital data processing asynchronous electronic circuitry based on self-timed elements, wherein the operating speed of the electronic circuitry is directly determined by its power supply voltage (see column 8, lines 41-46).

The feedback means controls the source of power supply voltage to vary the actual supply voltage provided to the electronic circuitry so as to dynamically control the data handling rate of the data source as a function of a filling degree signal reflecting the filling degree of a buffer storage means (see column 8, lines 50-60).

When replacing in the circuitry of Niessen the feedback control means which is responsive to the filling degree signal by a random generator or by a signal varying the supply voltage in a random way, then the desired filling degree control of Niessen would no longer work. Thus, there cannot be any reasonable expectation of success for one of ordinary skill to modify the circuitry of Niessen as proposed by the Examiner. Moreover, neither Niessen nor Dias contain any teaching or

suggestion that would motivate one skilled in the present field to replace the filling degree feedback control for the buffer storage means of Niessen by a random signal.

The Examiner's argument outlined in the penultimate sentence of page 2 of the final Office Action that even with a random signal as the filling degree signal the filling of the Niessen technique should still occur is technically incorrect. Clearly, the filling degree signal must reflect the filling degree of the buffer storage means (column 8, lines 50-60). If the filling degree signal varies in a random way rather than reflecting the filling degree of the buffer storage means, then the buffer storage means would either run empty or would be over-filled. Thus, one skilled in the present field would necessarily understand that any feedback control signal in the technique of Niessen which does not reflect the filling degree of the buffer storage means would render the technique of Niessen technically useless. A technically useless control which can neither prevent the running-empty of the buffer storage means nor prevent an overfilling thereof would not be taken into consideration as a reasonable replacement of Niessen's technique to make use of a feedback signal reflecting the filling degree of the buffer storage means.

Thus, independent claims 1 and 3, along with dependent claims 5-10, are patentable over the applied references for at least these reasons.